

DEP Documentation

DEP Quick Load Guide

Version Management Report			
Version	Name(s)	Date	Comments
xx.xx	F. Bormans	xx/xx/xxxx	Initial version
03.00	F. Demaertelaere	11/07/2005	Reformatting

COPYRIGHT NOTICE

The information contained in this document is subject to change without notice. *banksys* assumes no responsibility for any errors or omissions that may appear in this document. The contents of this document must not be reproduced in any form whatsoever, by or on behalf of third parties, without prior written consent of *banksys*.

1. TABLE OF CONTENTS

1. TABLE OF CONTENTS.....	3
2. SCOPE OF THE DOCUMENT	4
3. REFERENCES.....	4
4. DEP QUICK LOAD GUIDE	4
4.1. PRELIMINARY	4
4.2. RESTORE BANKSYS AUTHORITY BY USING THE BANKSYS DCC	5
4.3. RESTORE CUSTOMER AUTHORITY BY CUSTOMER.....	5
4.4. READ REQUIRED KEY TAGS FROM DCC LIST.....	6
4.5. SOFTWARE LOADING	6
4.6. KEY BACKUP LOADING.....	7
4.7. LOAD REQUIRED CAPABILITIES IN DEP CRYPTO MODULE.....	8
4.8. POST PROCESSING.....	8
4.9. REMARKS.....	9

2. SCOPE OF THE DOCUMENT

The DEP Quick Load Guide describes step-by-step the procedure how to load a DEP/PCI with software and keys.

This guide cannot be generalized because the procedure depends on some definitions of the Customer's Security Officer (such as secret sharing). The guide is written as an example (and should thus be adapted when necessary).

A complete and generic procedure can be found in the document *DEP Customer's Security Officer's Guide*.

See the manual *DEP C-ZAM/DEP User Manual* for more information about all the C-ZAM/DEP actions.

3. REFERENCES

This document contains a reference to other documents about the DEP. This paragraph gives a list of all the documents referred to.

- *DEP/NT DEP Handler Supervision User Manual*
- *DEP Customer's Security Officer's Guide*
- *DEP C-ZAM/DEP User Manual*

There are no references made to the following documents, but they could be useful to understand this document.

- *DEP Introduction to DEP*
- *DEP General Architecture*
- *DEP Glossary*

4. DEP QUICK LOAD GUIDE

4.1. PRELIMINARY

NOTE: Make sure that the on the module you want to work with, the battery is set "on". It can be done with the DEP Handler Supervision via: *DEPx – Reset Functions – Set Battery On* (see document *DEP/NT DEP Handler Supervision User Manual* for more information).

➡ SWITCH THE DEP CRYPTO MODULE OFF LINE

4.2. RESTORE BANKSYS AUTHORITY BY USING THE BANKSYS DCC

- ➡ C-ZAM/DEP: SELECT: **BANKSYS AUTHORITY**
- ➡ C-ZAM/DEP: SELECT: RESTORE BANKSYS AUTHORITY
- ➡ CHOOSE MODE: USE '↑ BUTTON' (TST = TEST; LIV = LIVE)
- ➡ ENTER CUSTOMER ID: *see on DCC*
- ➡ READ CZD LISTS FROM DCC: 'OK'
- ➡ INSERT DEF DCC: INSERT DCC DEFINITION LIST
- ➡ READING...
- ➡ LIST READ FROM DCC: 'OK'
- ➡ REMOVE DCC: REMOVE DCC
- ➡ GET **KEY KM_AUTH_BKS**: 'OK'
- ➡ INSERT STO DCC: INSERT DCC STORAGE
- ➡ SEARCHING...
- ➡ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➡ READING...
- ➡ KEY PART READ FROM DCC: 'OK'
- ➡ REMOVE DCC: REMOVE DCC
- ➡ KEY RECONSTRUCTED: 'OK'
- ➡ BKS AUTHORITY RESTORED: 'OK'
- ➡ STOP....STOP...STOP.....
- ➡ C-ZAM/DEP: SELECT: CAPABILITIES
- ➡ C-ZAM/DEP: SELECT: ACTIVATE CZD CAPABILITY
- ➡ CAPABILITY **CAP_CUST_AUTH**: USE '↑' AND 'OK'
- ➡ SELECTED CAP...
- ➡ INSERT STO DCC: INSERT DCC STORAGE
- ➡ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➡ READING...
- ➡ CAP PART READ FROM DCC: 'OK'
- ➡ REMOVE DCC: REMOVE DCC
- ➡ CAP READ FROM DCC...
- ➡ CAPABILITY ACTIVATED: 'OK'
- ➡ STOP – STOP – STOP...

4.3. RESTORE CUSTOMER AUTHORITY BY CUSTOMER

- ➡ C-ZAM/DEP: SELECT: **CUSTOMER AUTHORITY**
- ➡ C-ZAM/DEP: SELECT: RESTORE CUSTOMER AUTHORITY
- ➡ GET **KEY KM_AUTH_CUST**: 'OK'
- ➡ INSERT STO DCC: INSERT DCC STORAGE
- ➡ SEARCHING...
- ➡ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➡ READING...
- ➡ KEY PART READ FROM DCC: 'OK'
- ➡ REMOVE DCC: REMOVE DCC
- ➡ KEY RECONSTRUCTED: 'OK'

- ➡ CUST AUTHORITY RESTORED: 'OK'
- ➡ C-ZAM/DEP: SELECT: CUSTOMER AUTHORITY
- ➡ CONNECT NOW C-ZAM/DEP TO DEP CRYPTO MODULE
- ➡ C-ZAM/DEP: SELECT: **CUSTOMER INIT DEP**
- ➡ INITIALIZING...
- ➡ DEP INITIALIZED: 'OK'

4.4. READ REQUIRED KEY TAGS FROM DCC LIST

- ➡ C-ZAM/DEP: SELECT: DEFINITION LISTS
- ➡ C-ZAM/DEP: SELECT: READ LISTS FROM DCC
- ➡ INSERT DEF DCC: INSERT DCC LIST
- ➡ READING...
- ➡ LIST READ FROM DCC: 'OK'
- ➡ REMOVE DCC: REMOVE DCC

4.5. SOFTWARE LOADING

- ➡ OPEN WIN/NT EXPLORER: SELECT: **DEP\APPLICATIONS....**
- ➡ OPEN THE <SOFTWARENAME>.SAC
- ➡ COPY THE SWAC CORRESPONDING TO THE CUSTOMER ID AND MODE
(USE COPY/PAST FUNCTION OF WINDOWS ONLY)
- ➡ C-ZAM/DEP: SELECT: CAPABILITIES
- ➡ C-ZAM/DEP: SELECT: ACTIVATE DEP CAPABILITY
- ➡ CAPABILITY **STD_SW_LOAD (05000300)**: USE 'UP'/'DOWN' AND 'OK'
- ➡ SELECTED CAP...
- ➡ INSERT STO DCC: INSERT DCC STORAGE
- ➡ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➡ READING...
- ➡ CAP PART READ FROM DCC: 'OK'
- ➡ REMOVE DCC: REMOVE DCC
- ➡ CAP READ FROM DCC...
- ➡ CHOOSE TYPE OF LIMITATION / UNLIMITED CAPABILITY: 'OK'
- ➡ ACTIVATING...
- ➡ CAPABILITY ACTIVATED: 'OK'
- ➡ ON THE DEP HANDLER SUPERVISION SELECT: DEP_x – **LOAD APPLICATION**
- ➡ SELECT <SOFTWARENAME>.**HEX** FILE
- ➡ PASTE THE SWAC (USE COPY/PAST FUNCTION OF WINDOWS ONLY)
- ➡ LOADING...
- ➡ READ STATUS...

4.6. KEY BACKUP LOADING

- ➔ C-ZAM/DEP: SELECT: **CAPABILITY**
- ➔ C-ZAM/DEP: SELECT: ACTIVATE DEP CAPABILITY
- ➔ CAPABILITY C_SAVE_KEYS (05000000): USE 'UP'/'DOWN' AND 'OK'
- ➔ SELECTED CAP...
- ➔ INSERT STO DCC: INSERT DCC STORAGE
- ➔ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➔ READING...
- ➔ CAP PART READ FROM DCC: 'OK'
- ➔ REMOVE DCC: REMOVE DCC
- ➔ CAP READ FROM DCC...
- ➔ CHOOSE TYPE OF LIMITATION / UNLIMITED CAPABILITY: 'OK'
- ➔ ACTIVATING...
- ➔ CAPABILITY ACTIVATED: 'OK'
- ➔ STOP – STOP – STOP.....

- ➔ C-ZAM/DEP: SELECT: **KEYS**
- ➔ C-ZAM/DEP: SELECT: READ LOCAL KEY FROM DCC
- ➔ TYPE IN TAG: 'NO' (USE '↑ button')
- ➔ KEY DEP_DMK (04000000)
- ➔ SELECTED KEY...
- ➔ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➔ READING...
- ➔ KEY PART READ FROM DCC: 'OK'
- ➔ REMOVE DCC: REMOVE DCC
- ➔ INSERT STO DCC: INSERT STORAGE DCC
- ➔ SEARCHING...
- ➔ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➔ READING...
- ➔ KEY PART READ FROM DCC: 'OK'
- ➔ REMOVE DCC: REMOVE DCC
- ➔ INSERT STO DCC: INSERT STORAGE DCC
- ➔ SEARCHING...
- ➔ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➔ READING...
- ➔ KEY PART READ FROM DCC: 'OK'
- ➔ REMOVE DCC: REMOVE DCC
- ➔ KEY RECONSTRUCTED: 'OK'
- ➔ KEY READ FROM DCC: 'OK'

- ➔ C-ZAM/DEP: SELECT: **KEYS**
- ➔ C-ZAM/DEP: SELECT: SEND KEYS TO DEP
- ➔ C-ZAM/DEP: SELECT: SEND **ONE** KEY TO DEP
- ➔ KEY DEP_DMK
- ➔ SELECTED...
- ➔ SENDING...
- ➔ KEY SENT TO DEP: OK

- ➡ ON THE DEP HANDLER SUPERVISION SELECT: DEP_x - **RESTORE KEYS**
- ➡ SELECT KEY FILE (*.DAT)
- ➡ RESTORING...



ERASE A KEY FROM DEP...SELECTED KEY... ...DMK !!!!

4.7. LOAD REQUIRED CAPABILITIES IN DEP CRYPTO MODULE

IEPP: C_SCM_LOAD, C_PUR_PER_CARD

- ➡ C-ZAM/DEP: SELECT: ACTIVATE DEP CAPABILITY
- ➡ CAPABILITY xxx: USE 'UP'/'DOWN' AND 'OK'
- ➡ SELECTED CAP...
- ➡ INSERT STO DCC: INSERT DCC STORAGE
- ➡ ENTER YOUR PIN: PIN ENTRY + 'OK'
- ➡ READING...
- ➡ CAP PART READ FROM DCC: 'OK'
- ➡ REMOVE DCC: REMOVE DCC
- ➡ CAP READ FROM DCC...
- ➡ CHOOSE TYPE OF LIMITATION UNLIMITED CAPABILITY: 'OK'
- ➡ ACTIVATING...
- ➡ CAPABILITY ACTIVATED: 'OK'

4.8. POST PROCESSING

- ➡ SWITCH THE DEP CRYPTO MODULE OFF-LINE

4.9. REMARKS

- The RESTORE BANKSYS AUTHORITY and RESTORE CUSTOMER AUTHORITY should be done once per C-ZAM/DEP.
- When closing the C-ZAM/DEP with the following procedure, all the information is kept inside the C-ZAM/DEP (also DMKs).
 - ➡ C-ZAM/DEP: SELECT: SPECIAL FUNCTIONS
 - ➡ C-ZAM/DEP: SELECT: SAVE DATA + TERMINATE

This function should be used carefully for **LIVE C-ZAM/DEPs...(UNDER SUPERVISION OF THE CUSTOMER'S SECURITY OFFICER)**
- When closing the C-ZAM/DEP with the following procedure, all the data is lost inside the CZAM/DEP (such as capabilities, keys, ...). This means that this data should be reloaded when using the C-ZAM/DEP.
 - ➡ C-ZAM/DEP: SELECT: SPECIAL FUNCTIONS
 - ➡ C-ZAM/DEP: SELECT: TERMINATE CZD SESSION